The HIPAA Implementation Newsletter Issue #25 – January 11, 2002
Delays: Yes and No | Bankers | Security Patches | Homeland Security (4)
Web format with links at http://lpf.com/hipaa

Happy New Year! We just got back from a bicycle trip in New Zealand. A beautiful change of pace from today's business and the events of 9/11.

Please feel free to forward this newsletter to associates or colleagues you think may find it of interest. If you have received a forwarded copy, please feel free to subscribe, just click: mailto:hipaa@lpf.com?subject=subscribe

_____Status: Transaction Delay Signed_____

As expected, President Bush signed HR 3323 that allows covered entities to delay implementation of the Transactions and Code Sets Rule until October 16, 2003. There are strings.
http://lpf.com/hipaa/text.html#the-act-extension-transacstion-text

_____Status: No Delay for Confidentiality of Data_____

"'It's not a delay; it's an extension,' said William Braithwaite, who until last month was the key HHS official in charge of developing HIPAA regulations. 'And anyone who thinks they can relax and do nothing is going to be slapped upside the head.'

"One section of the just-passed legislation requires healthcare organizations to protect the confidentiality of patient data in business transactions by April 2003 whether data are transmitted in a HIPAA-compliant
format or some other way. … By writing that proviso into the law, Congress underscored its resolve to resist further lobbying efforts and guarantee protection of sensitive patient data in step with electronic standards, Braithwaite said.

"Braithwaite said the extension gives healthcare organizations only six additional months to get a workable transaction system in place because of the deadline of April 2003 for testing readiness. 'They can't test until they can conduct the transactions,' he said.

"The penalty for not meeting the planning and testing deadlines is possible exclusion from the Medicare program. But the real penalty looms at the end of the extension period when Medicare accepts only HIPAA-compliant healthcare claims from providers and health plans, Braithwaite said.

"'Thus they get a six-month period to test the transactions until the guillotine comes down,' he said. 'If you can't submit a claim and get it paid from Medicare, 80% of the (healthcare) system will shut down.'"
---December 24,2001 Modern Healthcare Magazine

http://www.modernhealthcare.com/currentissue/topten.php3?refid=8213&db=mh99u
p&published=20011224

_____Have You Talked With Your Banker?____

If you are using a "lockbox" service provided by your bank or someone else to process payments, they may have access to EOB (explanation of benefits) data according to an article published by the Privacy Officers Association. That may trigger the privacy and security regulations of HIPAA. In issue #5, we reported:

Nine federal agencies have responsibility for enforcing Gramm-Leach-Bliley. Five of the agencies have coordinated publication of regulations: Department of the Treasury, Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation and the Office of Thrift Supervision. [The agencies that regulate your bank.] … All of the agencies that have published rules have included something similar to the following quotation from the SEC in their final regulations. The definition of "financial information" covered by the Act, "is extremely broad and may include, for instance, medical information and other types of information that might not commonly be thought of as financial. … We recognize that there could be areas of overlap between the rules adopted by HHS under HIPAA and the privacy rules. After HHS publishes its final rules, we will consult with HHS to avoid the imposition of duplicative or inconsistent requirements." Privacy regulations for medical information clearly extend beyond health care providers and health insurance plans. Efforts are promised to coordinate the relevant regulations across industries.

To the extent that your banker is dealing with medical information, their regulatory agencies will probably make them meet the privacy and security requirements of HIPAA. Your banker or any other organization you use would also appear to meet the definition of a "business associate" i.e., "A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce." Either way, it is in your best interest to deal with this issue as early as possible.
-----http://www.wedi.org/public/articles/HIPAA_GLOSSARY.pdf
-----http://www.privacyassociation.org/docs/poa-news-sample.pdf

_____Security: Are Your Patches Current_____

"Now, I'm not a doctor, and I don't play one on television. And I'm not a chief security officer, but I will play one--however superficially--for the purposes of this column.

"My career shift was triggered by a news item that appeared late last week … about a security flaw in Solaris 8:'Security vendor Internet Security Systems Inc. is warning users of Sun Microsystems Solaris 8 and earlier versions that a serious vulnerability gives hackers 'super user' privileges. … According to an alert published by ISS, the vulnerability in the 'login' program in Solaris enables attackers to run arbitrary commands on a target system.'

"The story went on to add that while Sun declined to comment, Internet Security Systems' warning stated that 'Sun is aware of the vulnerability and is testing a fix. Patches may be available soon' And I wondered how soon those patches could be grabbed and installed by customers. Are we talking days? Weeks? And how many customers saw the independent advisory? Was Sun itself informing its customers?

"In this age of growing awareness of personal responsibility, what about the customer side: Once they know about the flaw and find out where and when to get the patches, how many IT departments will actually locate, download, install, monitor, and test the patches? All? Most? Half? And for those that don't, why not? Too much trouble? Not much risk? Not my job?

"So I took a look back at another story … on security and hackers that discussed a security flaw based not in the code but rather in that most complex of all programs: human behavior. …

"Clearly, some of the blame falls on IT managers for not installing publicly available patches. Hackers have been known to exploit vulnerabilities weeks, months, sometimes years after flaws have been made public and patches made available. Early last year, a hacker calling himself Curador stole more than 25,000 credit-card numbers from small E-commerce Web sites by exploiting a well-known Microsoft security flaw, even though the vendor had published a patch."

[The story] "went on to quote a network administrator with a major medical company who said, "Security often takes a backseat to other projects that management deems more important, and the resources aren't always made available to put patches into place immediately--or even within weeks."

"Back in the summer, Code Red infected more than 350,000 networks, crippled Web sites, and even managed to slow down overall Internet traffic. History, human nature, and a combination of technological progress and technical limitations offer us more than ample evidence to believe Code Red won't be the last wide scale virus, nor will it be the most destructive. All of those points would seem to require a dramatic reordering of priorities in companies where, as noted in the quote above, security is mostly an afterthought.

“For you CIOs and chief security officers out there: Is patch installation a priority in your company? Is it talked about and hyped, or is it truly valued? Is it part of a compensation package? Do you keep a list of flaws, availability of patches, and installation of patches? Do you want to face the CEO when she asks, ‘You mean we knew about this virus but didn't inoculate ourselves?’”

COMMENTARY: We do not give legal advice, but we cannot help but wonder what a plaintiff’s attorney would do with the same information in a suit alleging a breach of privacy and security by a plan or a provider.
----- http://www.informationweek.com/story/IWK20011214S0022

_____2002 Challenges_____

A poll by HealthLeaders magazine ranked “Terrorism Preparedness” and HIPAA as the two biggest challenges facing healthcare in 2002.

32%	Terrorism Preparedness
26%	HIPAA
22%	Staffing Shortages
16%	Financial Reimbursement
5%	Technology Adoption

Terrorism preparedness has also been a popular topic in the articles we read and the discussions we follow as suggested by the following articles. It’s not just HIPAA.
-----http://www.healthleaders.com/news/section.php?categoryid=35 Quick poll, “view the poll” as of 1/8/02

_____Not Just HIPAA: Homeland Defense_____

“Homeland security budgets are expected to receive yet another dramatic boost in the coming year. President Bush is expected to seek another $15 billion for homeland defense activities, while Congress is expected to press for even more. According to media reports, the White House hopes to double funding for local police, firefighters and other first responders, as well as provide **major increases in the budgets for public health agencies and hospitals.** Bush also will propose additional increases in spending for bioterrorism research and aviation security.”
-----Homeland Defense Journal
http://www.homelanddefensejournal.com/hdj_vol1_no1.pdf

_____Security: Experience Is In Demand_____

Staffing seems to be an “everywhere, all-the-time” issue in the healthcare industry. Just as healthcare organizations are ramping up to improve information security as required by HIPAA and physical security as required by the threat of terrorism, other organizations are competing for the limited supply of experienced security managers.

“The Department of Transportation has hired a major executive search firm to
help it begin hiring security directors for the nation's airports. Korn/Ferry International has been contracted to recruit candidates for federal security directors at 81 major airports. … By the end of the year, the new Transportation Security Agency is mandated to hire federal security directors for all 429 airports in the country… and other security personnel as it takes over direct responsibility for securing the nation's airports.
CNN January 9, 2002 Posted: 5:15 PM EST (2215 GMT)

In Issue #21, we noted a Wall Street Journal article by Laura Landro: “Attacks Demonstrate Need for US. Network Of Online Medical Files.” The two following articles report on recent calls for more online medical information and information systems.

_____National Health Information System_____

”To protect public health and national safety, the American Medical Informatics Association (AMIA) recommends that the federal government dedicate technological resources and medical informatics expertise to create a national health information infrastructure (NHII). An NHII provides the underlying information utility that connects local health providers and health officials through high-speed networks to national data systems (e.g., Centers for Disease Control and Prevention) necessary to detect and track global threats to public health. … [What is required? Two items related to HIPAA:]

“Standards - Effective communications among local, community, state and federal facilities require the use of standards. Healthcare messaging standards should be used for data interchange. A common vocabulary standard
and required data elements for public health surveillance databases are required to enable effective sharing of data. … Government coordination and support for consensus standardization and low-cost distribution of common vocabularies for health event detection, prevention, and intervention is a fundamental aspect of a national health information infrastructure.” HIPAA provides a model for how to do this.

“National identifiers - National identifiers for providers, insurers, businesses, and individuals are required by … HIPAA. The privacy provision of HIPAA that protects confidential health information has been finalized.

In the face of the acute crisis, the work on identifiers should be accelerated so that effective epidemiological data can be gathered and analyzed and appropriate health care services delivered where needed." Identifiers for individuals are way beyond the scope of this newsletter, but the other identifiers are reportedly to be in the home stretch of development.
-----American Medical Informatics Association Advocates National Health Information System in Fight Against National Health Threats
http://www.amia.org/

_____RAND: Bioterrorism Preparedness_____

"On November 14, 2001, a Summit was convened by RAND's Science and Technology Policy Institute as part of its mission to address scientific and technological issues of national importance. The purpose of the Summit was to bring together a diverse set of stakeholders to begin the process of developing a conceptual framework needed for an IT infrastructure that could support bioterrorism preparedness efforts across the country. Cosponsors included the American College of Preventive Medicine and IEEE-USA Medical Technology Policy Committee.

"The massive devastation associated with the events of September 11th and subsequent anthrax episodes have heightened the urgency of meeting this challenge. A core element in biopreparedness is an IT infrastructure that enables the collection, analysis, and dissemination of critical information in real time to prevent or mitigate the effects on populations from a bioweapons event. This IT infrastructure does not exist." Technological issues cited included:

* Not capable of capturing health information from a population level
* Evidence of effectiveness
* Limited data
* Lack of quality and completeness of data
* Duplication of effort and resources
* Lack of scalability
* Unknown surge capabilities
* Lack of data on current infrastructure
* Incompatibility, lack of standards (e.g., vocabularies)

Again, HIPAA provides a beginning point and experience useful in moving forward. However, a nationwide system will add even more burden to an already burdened industry.
-----A Framework for the Information Technology Infrastructure for Bioterrorism
12/7/2001 http://www.rand.org/scitech/stpi/Infrastructure/summary.pdf

_____Update_____ A link to the Homeland Defense Journal has been added followed by Healthcare Humor, a healthcare cartoon weekly to the "news"

page
at: http://lpf.com/hipaa/news.html#homeland-defense-news A Disaster Recovery/Business Continuity section has been added to the "tools" page at: http://lpf.com/hipaa/tools.html#disaster-recovery-tools

____

To be removed from this mail list, click:
mailto:hipaa@lpf.com?subject=remove To subscribe, click:
mailto:hipaa@lpf.com?subject=subscribe We appreciate it if you include information about your firm and your interests.

The HIPAA Implementation Newsletter is published periodically by Lyon, Popanz & Forester. Issues are posted on
the Web at http://lpf.com/hipaa concurrent with email distribution. Past issues are also available there. Edited by Hal Amens hal@lpf.com

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There
are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning, program management offices and project management for HIPAA are areas of
special interest.